

## REMARKS

Favorable reconsideration of this application, for the reasons Applicant respectfully submits hereinbelow, is respectfully requested.

Claims 1-8, 10-11 and new claims 12-16 are the only claims currently active in this application. Claim 9 is canceled, without prejudice and without any disclaimer of subject matter.

The foregoing separate sheets marked as "Listing of Claims" show all the claims in the application, each having an indication at its first line showing the claim's current status.

New independent claim 16 recites a method according to at least one of the exemplary embodiments. This claim is not new matter; exemplary support may be found at, for example, the Specification at page 6, lines 1-3 and at page 7, line 1, through page 8, line 13, and at original claim 9.

New dependent claims 17-22 are not new matter; each recites, in alternative language, subject matter encompassed by the original claims, additionally supported at, for example, page 8, line 8 through page 9, line 31 of the Specification.

The Office Action recites a rejection of claims 1-11 under 35 U.S.C. § 102(b), on the stated position that each claim is anticipated by U.S. Publication No. 2005/0089060 ("*Vergnes*"). *Id.*, at pages 2-8,

Applicant respectfully traverses all of these rejections, on the grounds that *Vergnes* lacks elements of each and every original claim of the present application.

**Claims 1 - 4**

Base claim 1 defines a first and a second combinatorial logic circuit, each having different logical operations performing the same function on the same input, in an arrangement dynamically selecting which of these logic circuits operates on that same input.

Applicant's Fig. 1 illustrates one of various disclosed examples supporting claim 1. Referring to Fig. 1, the example includes combinatorial logic circuits 101, 103 and 105 arranged to be dynamically selectable, by the selection circuit 111, the selector 107, and the merger circuit 109, to operate on the same data input 129. As described by Applicant's specification at, for example, page 8, line 7, through page 9, line 14, each of the combinatorial logic circuits 101, 103 and 105 performs the same overall function but with different logical operations. As described, this dynamic selection of combinatorial logic circuit provides resistance to power analysis.

Interpreting claim 1 according to its broadest reasonable meaning, *Vergnes* discloses nothing meeting the recited second combinatorial logic circuit, and nothing within meeting the recited arrangement for dynamically selecting between the first and second combinatorial logic circuit.

Further, without waiver of traversal or disclaimer of subject matter, Applicant has amended claim 1 for form, to more positively recite these distinguishing features.

Applicant now respectfully turns to the Examiner's statements of position regarding *Vergnes*.

At pages 2-3 of the Office Action the Examiner takes the position that *Vergnes* "combinatorial circuits" 412-1 and 412-2 meet the claim 1 first combinatorial logical circuit and second combinatorial logic circuit.

Applicant respectfully responds there at least two reasons under which *Vergnes* does not and cannot support the Examiner's position.

First, claim 1 recites the first and second combinational logic circuits as performing the same function with two different logical operations. Claim 1, currently amended, at lines, 16-17.

*Vergnes*, in sharp contrast, discloses *nothing* of circuits 412-1 and 412-2 performing the same function *with different logical operations*. *Vergnes* discloses nothing more than the *functions* of the circuits 412-1 and 412-2, with respect to DES cycles, may be the same. *See*, for example, *Vergnes* at paragraph 0033, last two lines. Applicant submits that disclosing that functions may be the same does *not* constitute a disclosure that, in addition to the functions being the same, the logical operations are *different*.

The second fact establishing that *Vergnes cannot* disclose the first and second combinational logic circuits of claim 1 is that these are recited as operating on the *same* input data. *See* claim 1, currently amended, at lines 11-12. *Vergnes'* circuit 412-2, in contrast, does not, and *cannot*, operate on the same input data as circuit 412-1 because the *Vergnes* combinatorial circuits 412-1 and 412-2 are *in series*.

Circuit 412-2 therefore *cannot* meet the claim 1 "second combinatorial logic circuit." because claim 1 recites that the circuit, if dynamically selected, operates on

the *same* input data as the first circuit would operate on if that circuit were selected.

*Vergnes* therefore *cannot*, for at least these two reasons stated above, anticipate Applicant's base claim 1.

Applicant respectfully requests, for at the reasons presented above, that the Examiner reconsider and withdraw the rejection of base claim 1.

Claims 2-4 depend from claim 1 and, for at least this reason alone, each is patentable over *Vergnes*.

Further, responding to the Examiner's statement that *Vergnes* meets the claim 2 language, Applicant respectfully refers to the example support at Applicant's Fig. 3. Applicant respectfully submits circuits 319 and 321 within block 301 as one example support meeting the claimed first and second combinatorial logic circuits, and to circuits 323 and 325 within block 303 as one example support meeting the claimed third and fourth combinatorial logic circuits.

Referring back to *Vergnes*, Applicant respectfully submits that *nothing* within that reference meets the claim 2 language.

Regarding claim 3, Example support is at Fig. 1, showing the selection circuit 111, the selector 107, and the merger circuit 109, to operate on the same data input 129. *Vergnes* lacks, for example, the selector because the *Vergnes* 412-1 circuit is the only one of the circuits 412-1 and 412-2 that can operate on the "in-data" 404. .

Regarding claim 4, *Vergnes* cannot meet its recited language because, for example, *Vergnes* lacks the base claim's second combinatorial logic circuit, as well as its recited arrangement relative other elements.

**Claims 5-8 and 10-11**

Base claim 5 defines a combinatorial logic circuit generating an output, an encoding means for encoding the output, a storage means for storing the encoded output, a decoding means corresponding to the encoding means for decoding the encoded output retrieved from the storage, and an electronic circuit dynamically control the activation of the first encoding means and the corresponding first decoding means.

Base claim 10 recites a method substantially corresponding to operations of the claim 5 apparatus.

Without waiver of traversal or disclaimer of subject matter, Applicant has amended claims 5 and 10 for form, to more clearly recite these and other distinguishing features.

Referring to Applicant's originally filed disclosure, at Fig. 4 and at the Specification at, for example, page 11, line 10, through page 12, line 30, illustrative example embodiments are shown that meet Applicant's claims 5 and 10. More particularly, for example, the Fig. 4 encoder 407 has a corresponding decoder 409 and, as described, these are dynamically enabled by circuitry including, for example, logic gates 413, 415, 417 and 419. The storage unit 401 stores the encoded

data, and the decoder 409 decodes that encoded data after retrieval. See Specification at page 11, line 10, through page 12, line 30

Turning now to *Vergnes*, the Examiner identifies this reference's Fig. 4, together with its paragraphs [0031] – [0036], [0046-0047] and [0051] as a disclosure of subject matter meeting the recited elements of claims 5 and 10. Office Action at pp. 3-4. Applicant respectfully responds that upon careful study of *Vergnes*' Fig. 4, and of *Vergnes*' paragraphs [0031] – [0036], [0046-0047] and [0051], Applicant cannot identify subject matter that a person of ordinary skill in the art pertaining to the invention would understand as being within the broadest reasonable meaning of the claim 5 or claim 10 recitation of encoding data prior to storing that data, combined with a unit decoding it after retrieval, with a dynamic control of the encoding and decoding.

Applicant submits that *Vergnes*, to the extent it can be understood, appears to describe a "storage element" 420 that is apparently controlled by mux 422 to store or not store intermediate processing results during encoding to increase or decrease the number of clock cycles required for the encoding or, when operating in a decoding mode, to store or not store intermediate processing results, so as to increase or decrease the number of clock cycles required for the decoding. Applicant respectfully submits that this subject matter fails to constitute disclosure of subject matter within the meaning of either of claims 5 or 10.

*Vergnes*, for at least the reasons presented above, cannot anticipate either of Applicant's base claims 5 or 10.

Applicant respectfully requests, for at the reasons presented above, that the Examiner reconsider and withdraw the rejection of base claims 5 and 10.

Claims 6-8 depend from claim 5 and claim 11 depends from claim 10 and, for at least these reasons alone, each of these claims is patentable over *Vergnes*.

#### **New Claims 12-22**

New dependent claims 12-15 and 17-22 recite further various distinguishing aspects, none of which are disclosed by *Vergnes*.

New claim 16 recites in alterative form a method of the disclosed invention corresponding generally to recited structural features of claim 1. Applicant therefore respectfully submits that claim 16 is patentable over the cited art for reasons including the reasons Applicant submits for claim 1.

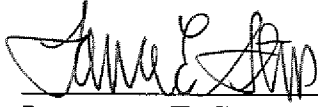
**CONCLUSION**

In view of the remarks above, Applicant believes that each of the rejections/objections has been overcome and the application is in condition for allowance. In the event that the fees submitted prove to be insufficient in connection with the filing of this paper, please charge our Deposit Account Number 50-0578 and please credit any excess fees to such Deposit Account.

Should there be any remaining issues that could be readily addressed over the telephone, the Examiner is asked to contact the agent overseeing the application file, Aaron Waxler, of NXP Corporation at (408) 474-5256.

Respectfully submitted,  
**KRAMER & AMADO, P.C.**

Date: January 14, 2010

  
\_\_\_\_\_  
Laurence E. Stein  
Registration No.: 35,371

Please direct all correspondence to:

Corporate Patent Counsel  
NXP Intellectual Property & Standards  
1109 McKay Drive; Mail Stop SJ41  
San Jose, CA 95131  
CUSTOMER NO.: 65913